(10) (5)文献

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-198530
(43)Date of publication of application : 11.07.2003

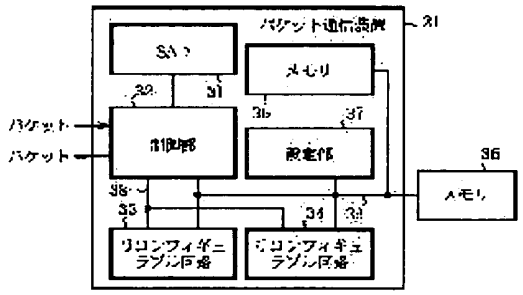
(51)Int.Cl. H04L 9/14

(21)Application number : 2001-390165
(22)Date of filing : 21.12.2001

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : KATO MAMORU

(54) PACKET COMMUNICATION DEVICE AND ENCRYPTION ALGORITHM SETTING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a packet communication device and an encryption algorithm setting method in which an encryption algorithm can be easily added or changed.
SOLUTION: A packet communication device 21 incorporates a setting part 37 for setting the circuit configuration date of reconfigurable circuits 33 and 34. Thus, there is an effect that the encryption algorithm can be easily added or changed.



LEGAL STATUS
[Date of request for examination] 15.11.2004
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] An algorithm decision means to check the destination of a packet and to determine cryptographic algorithm according to the destination, Cryptographic algorithm determined by the above-mentioned algorithm decision means is performed. In the packet communication device equipped with a processing activation means to perform encryption processing to the packet, and a transmitting means to transmit the packet after encryption by the above-mentioned processing activation means The packet communication device characterized by establishing a setting means to constitute the above-mentioned processing activation means using a recon figure skating rubble circuit, and to set up the circuitry data of the above-mentioned recon figure skating rubble circuit.
[Claim 2] A receiving means to receive the enciphered packet, and an algorithm decision means to check the transmitting origin of the packet received by the above-mentioned receiving means, and to determine cryptographic algorithm according to the transmitting origin, In the packet communication device equipped with a processing activation means to perform cryptographic algorithm determined by the above-mentioned algorithm decision means, and to perform decryption processing to the packet The packet communication device characterized by establishing a setting means to constitute the above-mentioned processing activation means using a recon figure skating rubble circuit, and to set up the circuitry data of the above-mentioned recon figure skating rubble circuit.
[Claim 3] A setting means is a packet communication device according to claim 1 or 2 characterized by registering the number of bits of the key length of a cryptographic key and encryption, or a decryption block in case the circuitry data of a recon figure skating rubble circuit are set up.
[Claim 4] The packet communication device according to claim 1 or 2 characterized by having the processing activation means which consisted of fixed hardware circuitry which performs predetermined cryptographic algorithm other than the processing activation means which consisted of recon figure skating rubble circuits.
[Claim 5] A setting means is a packet communication device according to claim 1 or 2 characterized by choosing the recon figure skating rubble circuit under un-performing, and setting up circuitry data when the processing activation means consists of two or more recon figure skating rubble circuits.
[Claim 6] A setting means is a packet communication device given [of claim 1 to the claims 5 which exchange the information about the communications partner and cryptographic algorithm of a packet, and are characterized by setting the circuitry data corresponding to the cryptographic algorithm to perform as a recon figure skating rubble circuit] in any 1 term.
[Claim 7] The setting means of a packet transmitting side is a packet communication device according to claim 6 characterized by transmitting the identifier which shows a purport equipped with the recon figure skating rubble circuit to the setting means of a packet receiving side, and transmitting the circuitry data corresponding to the cryptographic algorithm to perform to the setting means of a packet receiving side if the notice of a purport equipped with the recon figure skating rubble circuit is received from the setting means of the packet receiving side.

[Claim 8] The setting means of a packet receiving side is a packet communication device according to claim 7 characterized by receiving the circuitry data transmitted from the setting means of a packet transmitting side, and setting the circuitry data as a recon figure skating rubble circuit.
[Claim 9] The cryptographic algorithm setting approach which the circuitry data corresponding to the cryptographic algorithm which the above-mentioned packet transmitting side performs will be transmitted to the above-mentioned packet receiving side, and the packet receiving side will receive the circuitry data concerned, and will be set as a recon figure skating rubble circuit if a letter is answered in the notice of the purport which the packet receiving side received the identifier concerned, and equips with the recon figure skating rubble circuit while a packet transmitting side transmits the identifier which shows a purport equipped with the recon figure skating rubble circuit to a packet receiving side.
[Claim 10] The cryptographic algorithm setting approach that will transmit the cryptographic algorithm which the above-mentioned packet transmitting side performs to the above-mentioned packet receiving side, and the packet receiving side will receive and set up the cryptographic algorithm concerned if the packet receiving side receives the identifier concerned and answers a letter in the notice of the purport which can use a recon figure skating rubble code while a packet transmitting side transmits the identifier which shows a recon figure skating rubble code to a packet receiving side.
[Claim 11] The cryptographic algorithm setting approach according to claim 10 characterized by the cryptographic algorithm transmitted from a packet transmitting side being the script performed with the script activation engine of

a packet receiving side.

[Claim 12] The cryptographic algorithm setting approach according to claim 10 characterized by the cryptographic algorithm transmitted from a packet transmitting side being the software performed by the microprocessor of a packet receiving side.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the packet communication device and the cryptographic algorithm setting approach of making an addition and modification of cryptographic algorithm.
[0002]
[Description of the Prior Art] By development of telecom infrastructures, such as the Internet, VPN (Virtual Private Network) attracts attention instead of the communication link by the dedicated lines between the inside of a company, or a company etc. With encoding technology, it is the technique which uses the Internet available as an imagination dedicated line, and, as for VPN, IPSEC (Security Architecture for Internet Protocol) serves as a current criterion. In IPSEC, the cryptographic algorithm to be used is not fixed but, in addition to indispensable cryptographic algorithm DES (Data Encryption Standard) etc., the support of the algorithm of arbitration is possible.
[0003] Drawing 9 is the block diagram showing the conventional packet communication device, and is set to drawing. 1 For example, the packet communication device which is network security LSI, While SAD (SecurityAssociation Database) which stores the information which shows the cryptographic algorithm to which 11 can perform a communications partner, and 12 perform transmission and reception of a packet The control section which controls the cipher-processing circuits 13 and 14, and 13 perform cryptographic algorithm A. The cipher-processing circuit which performs the encryption processing or decryption processing to a packet, and 14 are cipher-processing circuits which perform cryptographic algorithm B and perform the encryption processing or decryption processing to a packet. In addition, although the example of drawing 9 shows that in which a packet communication device contains two cipher-processing circuits, it may not restrict to this, only one cipher-processing circuit may be built in, and three or more cipher-processing circuits may be built in.
[0004] Next, actuation is explained. Here, as shown in drawing 10 , packet communication device 1a which can perform cryptographic algorithms A and B enciphers a packet, and transmits, and that to which packet communication device 1b which can perform cryptographic algorithm A receives and decrypts a packet is explained.
[0005] First, in order that the control section 12 of packet communication device 1a may be faced starting the encryption communication link of a packet and may make packet communication device 1b of a receiving side recognize the cryptographic algorithm which can be performed, it transmits the identifier currently assigned to cryptographic algorithms A and B, respectively to packet communication device 1b.
[0006] The control section 12 of packet communication device 1b will recognize it as the cryptographic algorithms which can perform packet communication device 1a being cryptographic algorithms A and B, if the identifier of packet communication device 1a to cryptographic algorithm A and the identifier of cryptographic algorithm B are received. And the control section 12 of packet communication device 1b relates with the address of packet communication device 1a etc., and stores the decision information concerned in SAD11 while it transmits the decision information to which use of cryptographic algorithm A is permitted to packet communication device 1a, since the cryptographic algorithm which can perform self among cryptographic algorithms A and B is cryptographic algorithm A.
[0007] If the decision information to which use of packet communication device 1b to cryptographic algorithm A is permitted is received, the control section 12 of packet communication device 1a relates with the address of packet communication device 1b etc., and stores the decision information concerned in SAD11. And if the packet of the plaintext which transmits to packet communication device 1b is inputted, the control section 12 of packet communication device 1a will use as a key the address added to the packet, will acquire decision information from SAD11, and will recognize the cryptographic algorithm used from the decision information. In this example, it is recognized as what uses cryptographic algorithm A.
[0008] Since the cryptographic algorithm to be used is cryptographic algorithm A, the control section 12 of packet communication device 1a outputs the packet of a plaintext to the cipher-processing circuit 13 which builds in cryptographic algorithm A. Thereby, the cipher-processing circuit 13 performs cryptographic algorithm A, carries out encryption processing to the packet of a plaintext, and outputs the packet after encryption to a control section 12. The control section 12 of packet communication device 1a transmits the packet after encryption to packet communication device 1b.
[0009] If the packet after encryption is received from packet communication device 1a, the control section 12 of packet communication device 1b will use as a key the address added to the packet, will acquire decision information from SAD11, and will recognize the cryptographic algorithm used from the decision information. In this example, it is

recognized as what uses cryptographic algorithm A.
[0010] Since the cryptographic algorithm to be used is cryptographic algorithm A, the control section 12 of packet communication device 1b outputs the packet after encryption to the cipher-processing circuit 13 which builds in cryptographic algorithm A. Thereby, the cipher-processing circuit 13 performs cryptographic algorithm A, carries out decryption processing to the packet after encryption, and outputs the packet of a plaintext to a control section 12. The control section 12 of packet communication device 1b carries out the external output of the packet of a plaintext.
[0011]
[Problem(s) to be Solved by the Invention] Since the conventional packet communication device was constituted as mentioned above, even if it could not use it but more powerful cryptographic algorithm was newly devised, unless did not design LSI which is newly hardware and it was manufactured, the technical problem which cannot be used occurred except the cryptographic algorithm which both the transmitting side and the receiving side build in.
[0012] In addition, in case a packet communication device performs the encryption communication link of a packet, to JP,10-257120,A, the script equivalent to cryptographic algorithm is acquired from the database connected to the network, and the technique in which the script activation engine of a packet communication device performs the script concerned is indicated. However, there are problems, like there is possibility that cryptographic algorithm will flow out by an internal crime etc. at the same time the high morals of a server management organization are called for, since the high cryptographic algorithm of the secrecy nature which should be used only between specific packet communication devices in this case is registered into a database. Moreover, since it is necessary to carry out encryption processing etc. while a script activation engine interprets the semantics of a script, there is also a problem to which rates, such as encryption processing, become slow compared with the packet communication device with which hardware was mounted.
[0013] It was made in order that this invention might solve the above technical problems, and it aims at acquiring the packet communication device and the cryptographic algorithm setting approach of making an addition and modification of cryptographic algorithm easily.
[0014]
[Means for Solving the Problem] The packet communication device concerning this invention is faced enciphering a packet and transmitting, and a setting means to set up the circuitry data of a recon figure skating rubble circuit is established.
[0015] The packet communication device concerning this invention is faced receiving a packet and decrypting, and a setting means to set up the circuitry data of a recon figure skating rubble circuit is established.
[0016] In case the packet communication device concerning this invention sets up the circuitry data of a recon figure skating rubble circuit, it registers the number of bits of the key length of a cryptographic key and encryption, or a decryption block.
[0017] The packet communication device concerning this invention is equipped with the processing activation means which consisted of fixed hardware circuitry which performs predetermined cryptographic algorithm other than the processing activation means which consisted of recon figure skating rubble circuits.
[0018] When the processing activation means consists of two or more recon figure skating rubble circuits, the packet communication device concerning this invention chooses the recon figure skating rubble circuit under un-performing, and sets up circuitry data.
[0019] The packet communication device concerning this invention exchanges the information about the communications partner and cryptographic algorithm of a packet, and sets the circuitry data corresponding to the cryptographic algorithm to perform as a recon figure skating rubble circuit.
[0020] The packet communication device concerning this invention transmits the identifier which shows the purport which the setting means of a packet transmitting side equips with the recon figure skating rubble circuit to the setting means of a packet receiving side, and if the notice of the purport equipped with the recon figure skating rubble circuit from the setting means of that packet receiving side is received, it will transmit the circuitry data corresponding to the cryptographic algorithm to perform to the setting means of a packet receiving side.
[0021] The setting means of a packet receiving side receives the circuitry data transmitted from the setting means of a packet transmitting side, and the packet communication device concerning this invention sets that circuitry data as a recon figure skating rubble circuit.
[0022] If a letter is answered in the notice of the purport which that packet receiving side received the identifier concerned, and equips with the recon figure skating rubble circuit while a packet transmitting side transmits the identifier which shows a purport equipped with the recon figure skating rubble circuit to a packet receiving side, the cryptographic algorithm setting approach concerning this invention transmits the circuitry data corresponding to the cryptographic algorithm which a packet transmitting side performs to a packet receiving side, and that packet receiving side will receive the circuitry data concerned, and will set it as a recon figure skating rubble circuit.
[0023] If that packet receiving side receives the identifier concerned and answers a letter in the notice of the purport which can use a recon figure skating rubble code while a packet transmitting side transmits the identifier which shows a recon figure skating rubble code to a packet receiving side, the cryptographic algorithm setting approach concerning this invention transmits the cryptographic algorithm which a packet transmitting side performs to a packet receiving side, and that packet receiving side will receive the cryptographic algorithm concerned, and will set it up.
[0024] It is made for the cryptographic algorithm setting approach concerning this invention to be a script with

which cryptographic algorithm transmitted from a packet transmitting side is performed with the script activation engine of a packet receiving side.

[0025] It is made for the cryptographic algorithm setting approach concerning this invention to be software with which cryptographic algorithm transmitted from a packet transmitting side is performed by the microprocessor of a packet receiving side.

[0026]

[Embodiment of the Invention] Hereafter, one gestalt of implementation of this invention is explained.

Gestalt 1. drawing 1 of operation is the block diagram showing the packet communication device by the gestalt 1 of implementation of this invention, and is set to drawing. While SAD which stores the information which shows the packet communication device whose 21 is for example, the network security LSI, and the cryptographic algorithm to which 31 can perform a communications partner, and 32 perform transmission and reception of a packet It is the control section (a transmitting means, receiving means) which checks destination [of a packet], or transmitting origin and determines cryptographic algorithm according to destination or transmitting origin. In addition, the algorithm decision means consists of SAD31 and a control section 32.

[0027] 33 and 34 perform cryptographic algorithm determined by the control section 32, it is the recon figure skating rubble circuit (processing activation means) which performs the encryption processing or decryption processing to the packet, and the recon figure skating rubble circuits 33 and 34 are constituted using techniques, such as FPGA and CPLD. 35, the memory in which 36 stores the key length of a cryptographic key, and the circuitry data of the number of bits of an encryption block, or the recon figure skating rubble circuits 33 and 34, The setting section to which 37 sets the circuitry data of the recon figure skating rubble circuits 33 and 34 (setting means), 38 connects between the recon FIGYU rubble circuit 33 and 34 with a control section 32. The encryption circuit bus which transmits the packet set as the object of encryption, and 39 are setting buses which connect between a control section 32, the recon FIGYU rubble circuits 33 and 34, the setting section 37 and memory 35, and 36, and transmit the circuitry data of the recon figure skating rubble circuits 33 and 34 etc.

[0028] In addition, as memory 35 and 36, nonvolatile memory, such as a flash memory, EEPROM, and a mask ROM, and volatile memory, such as RAM, are usable, for example. In order to build in LSI like memory 35 for area saving, to choose much cryptographic algorithm and to make mounting possible, it is good also as external like memory 36. Moreover, it is also possible by mounting the both to hold standard cryptographic algorithm fixed by the internal mask ROM, and to offer the cryptographic algorithm of an option by memory cards, such as an external flash memory and CompactFlash (R). Moreover, although the example of drawing 1 shows that in which a packet communication device contains two recon figure skating rubble circuits, it may not restrict to this, only one recon figure skating rubble circuit may be built in, and three or more recon figure skating rubble circuits may be built in.

[0029] Next, actuation is explained. First, when performing modification and the addition of cryptographic algorithm which the packet communication device 21 performs, the setting section 37 will acquire the circuitry data of the recon figure skating rubble circuit stored in memory 35 or memory 36, if LSI is reset. In addition, circuitry data are stored in drawing 2 together with attribute information, such as the identifier and the key length of a cryptographic key who show corresponding cryptographic algorithm, and the number of bits of an encryption block, so that it may be shown.

[0030] And the setting section 37 will set the circuitry data as the recon figure skating rubble circuit 33, if the circuitry data of a recon figure skating rubble circuit are acquired. Thereby, if the circuitry data is circuitry data of for example, cryptographic algorithm B, as for the recon figure skating rubble circuit 33, activation of cryptographic algorithm B will be attained henceforth.

[0031] In addition, when the control section 32 of the packet communication device 21 is performing communication link actuation, if circuitry data are acquired from memory 35 or memory 36, the setting section 37 will choose the recon figure skating rubble circuit of the direction which has not carried out current activation among the recon figure skating rubble circuits 33 and 34, and will set up circuitry data to the recon figure skating rubble circuit.

[0032] Here, although a control section 32 transmits a packet to the recon figure skating rubble circuit 33 through the encryption circuit bus 38 in case it requests encryption processing and decryption processing of a packet to the recon figure skating rubble circuit 33, it reads the key length of a cryptographic key and the number of bits of an encryption block which are stored in memory 35 or memory 36. And temporarily, when the key length of a cryptographic key and the number of bits of an encryption block are larger than the bit width of face of the encryption circuit bus 38, it transmits by dividing into multiple times. For example, by 64 bits, the bit width of face of the encryption circuit bus 38 transmits a cryptographic key in 2 steps, when the key length is 128 bits. By this, cryptographic algorithm of the arbitration from which the key length and the number of bits of a block differ can be mounted in a recon FIGYU rubble circuit.

[0033] Next, as shown in drawing 3 , packet communication device 21a which can perform standard cryptographic algorithm A (for example, DES) explains the actuation in the case of transmitting a packet to packet communication device 21b which can perform cryptographic algorithm A (the example 1 of operation is called hereafter).

[0034] First, the control section 32 of packet communication device 21a transmits the identifier A currently assigned to cryptographic algorithm A to packet communication device 21b in order to make packet communication device 21b of a receiving side recognize the cryptographic algorithm which can be performed. The control section 32 of packet communication device 21b relates with the address of packet communication device 21a etc., and stores the decision information concerned in SAD31 while it will transmit the decision information to which use of cryptographic algorithm A is permitted to packet communication device 21a since self is possible for activation of

cryptographic algorithm A if the identifier A of packet communication device 21a to cryptographic algorithm A is received.

[0035] If the decision information to which use of packet communication device 21b to cryptographic algorithm A is permitted is received, the control section 32 of packet communication device 21a relates with the address of packet communication device 21b etc., and stores the decision information concerned in SAD31. And if the packet of the plaintext which transmits to packet communication device 21b is inputted, the control section 32 of packet communication device 21a will use as a key the address added to the packet, will acquire decision information from SAD31, and will recognize the cryptographic algorithm used from the decision information. In this example, it is recognized as what uses cryptographic algorithm A.

[0036] Since the cryptographic algorithm to be used is cryptographic algorithm A, the control section 32 of packet communication device 21a outputs the packet of a plaintext to the recon FIGYU rubble circuit (here, the recon FIGYU rubble circuit 33 considers as the thing of explanation which can perform cryptographic algorithm A for convenience) which can perform cryptographic algorithm A. Thereby, the recon FIGYU rubble circuit 33 performs cryptographic algorithm A, carries out encryption processing to the packet of a plaintext, and outputs the packet after encryption to a control section 32. The control section 32 of packet communication device 21a transmits the packet after encryption to packet communication device 21b.

[0037] If the packet after encryption is received from packet communication device 21a, the control section 32 of packet communication device 21b will use as a key the address added to the packet, will acquire decision information from SAD31, and will recognize the cryptographic algorithm used from the decision information. In this example, it is recognized as what uses cryptographic algorithm A.

[0038] Since the cryptographic algorithm to be used is cryptographic algorithm A, the control section 32 of packet communication device 21b outputs the packet after encryption to the recon FIGYU rubble circuit (here, the recon FIGYU rubble circuit 33 considers as the thing of explanation which can perform cryptographic algorithm A for convenience) which can perform cryptographic algorithm A. Thereby, the recon FIGYU rubble circuit 33 performs cryptographic algorithm A, carries out decryption processing to the packet after encryption, and outputs the packet of a plaintext to a control section 32. The control section 32 of packet communication device 21b carries out the external output of the packet of a plaintext.

[0039] Next, as shown in drawing 4 , packet communication device 21a which can perform standard cryptographic algorithm A explains actuation in case the circuitry data of cryptographic algorithm A transmit a packet to non-set up packet communication device 21b to a recon FIGYU rubble circuit (the example 2 of operation is called hereafter). However, since cryptographic algorithm A is a standard code (for example, DES), the circuitry data of cryptographic algorithm A shall be beforehand stored in memory 35.

[0040] First, the control section 32 of packet communication device 21a transmits the identifier A currently assigned to cryptographic algorithm A to packet communication device 21b in order to make packet communication device 21b of a receiving side recognize the cryptographic algorithm which can be performed. If the identifier A of packet communication device 21a to cryptographic algorithm A is received, since the circuitry data of cryptographic algorithm A are not set as the recon FIGYU rubble circuit 33 to build in, the control section 32 of packet communication device 21b requires a setup of the circuitry data of cryptographic algorithm A of the setting section 37.

[0041] Thereby, the setting section 37 of packet communication device 21b acquires the circuitry data of cryptographic algorithm A from memory 35, and sets the circuitry data as the recon FIGYU rubble circuit 33. The control section 32 of packet communication device 21b relates with the address of packet communication device 21a etc., and stores the decision information concerned in SAD31 while it will transmit the decision information to which use of cryptographic algorithm A is permitted to packet communication device 21a, if a setup of the circuitry data based on the setting section 37 is completed.

[0042] If the decision information to which use of packet communication device 21b to cryptographic algorithm A is permitted is received, the control section 32 of packet communication device 21a relates with the address of packet communication device 21b etc., and stores the decision information concerned in SAD31. Since the following communication link actuation is the same as that of the above-mentioned example 1 of operation, explanation is omitted.

[0043] Next, as shown in drawing 5 , packet communication device 21a which can perform cryptographic algorithm B newly devised as standard cryptographic algorithm A explains the actuation in the case of transmitting a packet to packet communication device 21b which can perform cryptographic algorithm A (the example 3 of operation is called hereafter). However, since cryptographic algorithm B is the newly devised code, the circuitry data of cryptographic algorithm B shall not be stored in memory 35.

[0044] First, the control section 32 of packet communication device 21a transmits the identifier A currently assigned to cryptographic algorithm A and the identifier R (or identifier which shows the purport which can use a recon FIGYU rubble code) which shows the purport which self equips with the recon FIGYU rubble circuit to packet communication device 21b in order to make packet communication device 21b of a receiving side recognize the cryptographic algorithm which can be performed. The control section 32 of packet communication device 21b will transmit the response R of the purport which self also equips with the recon FIGYU rubble circuit (or response of the purport which self can also use [of a recon FIGYU rubble code]) to packet communication device 21a, if the identifier R other than the identifier A of packet communication device 21a to cryptographic algorithm A is received.

[0045] However, when packet communication device 21b is not equipped with the recon FIGYU rubble circuit, the decision information to which use of cryptographic algorithm A is permitted is transmitted to packet communication device 21a. In this case, since the following communication link actuation is the same as that of the above-mentioned example 1 of operation, explanation is omitted.
[0046] In order to enable use of the code newly devised as the control section 32 of packet communication device 21a receiving the response R of the purport which self also equips with the recon FIGYU rubble circuit from packet communication device 21b, the circuitry data of cryptographic algorithm B are transmitted to packet communication device 21b. The control section 32 of packet communication device 21b will set the circuitry data of cryptographic algorithm B as a vacant recon FIGYU rubble circuit (for example, recon FIGYU rubble circuit 34), if the circuitry data of packet communication device 21a to cryptographic algorithm B are received.
[0047] In addition, when there is no vacant recon FIGYU rubble circuit, they enables it to use any one recon FIGYU rubble circuit for cancelling the recon FIGYU rubble circuit which mounts the circuitry data of cryptographic algorithm with the for example lowest operating frequency etc. according to the nullification algorithm generally considered, making it into an opening compulsorily.
[0048] The control section 32 of packet communication device 21b relates with the address of packet communication device 21a etc., and stores the decision information concerned in SAD31 while it will transmit the decision information to which use of cryptographic algorithm B is permitted to packet communication device 21a, if a setup of circuitry data is completed.
[0049] If the decision information to which use of packet communication device 21b to cryptographic algorithm B is permitted is received, the control section 32 of packet communication device 21a relates with the address of packet communication device 21b etc., and stores the decision information concerned in SAD31. Since the following communication link actuation is the same as that of the above-mentioned example 1 of operation, explanation is omitted.
[0050] Since it constituted above according to the gestalt 1 of this operation so that the setting section 37 which sets up the circuitry data of the recon figure skating rubble circuits 33 and 34 might be formed so that clearly, it is effective in the ability to make an addition and modification of cryptographic algorithm easily. Moreover, since a transmitting side and a receiving side do not need to transmit the circuitry data of cryptographic algorithm and do not need to register cryptographic algorithm into a database like the conventional example by communication link of one to one, it is effective in the secrecy nature of cryptographic algorithm being securable. In addition, since the recon figure skating rubble circuits 33 and 34 are hardware, delay of processing speed like the conventional script activation engine does not become a problem.
[0051] Especially with the gestalt 1 of this operation, when two or more packet communication devices are connected to the network, an IP address is assigned to two or more packet communication devices, although reference is not made, in case a transmitting side adds an IP address to a packet and transmits to it, it transmits to that packet including the circuitry data of cryptographic algorithm, and a receiving side stores the circuitry data concerned in memory 35. Thereby, a certain packet communication device can add cryptographic algorithm to other packet communication devices.
[0052] In case an identifier, circuitry data of cryptographic algorithm, etc. in which the cryptographic algorithm which can be performed is shown are transmitted, it enciphers, for example by standard encryption algorithm, and you may make it transmit the identifier and circuitry data especially with the gestalt 1 of the gestalt 2. above-mentioned implementation of operation, although reference is not made. Moreover, although the gestalt 1 of the above-mentioned implementation showed what sets up the circuitry data of cryptographic algorithm, a transmitting side transmits attribute information, such as the key length of a cryptographic key, and the number of bits of an encryption block, to a receiving side, and you may make it store the attribute information in the memory 35 of a receiving side. Thereby, the key length of a cryptographic key, the number of bits of an encryption block, etc. can be changed.
[0053] Gestalt 3. drawing 6 of operation is the block diagram showing the packet communication device by the gestalt 3 of implementation of this invention, and in drawing, since it shows that the same sign as drawing 1 is the same, or a considerable part, it omits explanation. 40 is a cipher-processing circuit (processing activation means) which is fixed hardware circuitry which performs predetermined cryptographic algorithm.
[0054] Next, actuation is explained. Although the gestalt 1 of the above-mentioned implementation showed what carries two or more recon figure skating rubble circuits, you may make it carry the cipher-processing circuit 40 other than the recon figure skating rubble circuit 34, as shown in drawing 6 . Mounting by specification, such as IPSEC, becomes possible [mounting indispensable cryptographic algorithm in the minimum amount of hardware] by this (the cryptographic algorithm concerned is mounted in the cipher-processing circuit 40), and the effectiveness that low cost-ization is realizable is done so.
[0055] As shown in drawing 7 , when the script activation engine of packet communication device 21b which is a receiving side performs cryptographic algorithm, you may make it the cryptographic algorithm transmitted from packet communication device 21a which is a transmitting side be the script performed with the script activation engine, although the gestalt 1 of the gestalt 4. above-mentioned implementation of operation showed what transmits the circuitry data of cryptographic algorithm. Thereby, also in the packet communication device of a script method, the same effectiveness as the gestalt 1 of the above-mentioned implementation can be done so.
[0056] As shown in drawing 8 , when the microprocessor of packet communication device 21b which is a receiving side performs cryptographic algorithm, you may make it the cryptographic algorithm transmitted from packet

communication device 21a which is a transmitting side be the software performed by the microprocessor, although the gestalt 1 of the gestalt 5. above-mentioned implementation of operation showed what transmits the circuitry data of cryptographic algorithm. Thereby, also in the packet communication device of the software method by the microprocessor, the same effectiveness as the gestalt 1 of the above-mentioned implementation can be done so.

[0057]

[Effect of the Invention] As mentioned above, since according to this invention it constituted so that a setting means to face enciphering a packet and transmitting and to set up the circuitry data of a recon figure skating rubble circuit might be established, it is effective in the ability to make an addition and modification of cryptographic algorithm easily.

[0058] Since according to this invention it constituted so that a setting means to face receiving a packet and decrypting and to set up the circuitry data of a recon figure skating rubble circuit might be established, it is effective in the ability to make an addition and modification of cryptographic algorithm easily.

[0059] Since according to this invention it constituted so that the number of bits of the key length of a cryptographic key and encryption, or a decryption block might be registered when setting up the circuitry data of a recon figure skating rubble circuit, it is effective in performing an addition and being able to make a change easily, also about the key length of a cryptographic key, or the number of bits of encryption or a decryption block.

[0060] Since according to this invention it constituted so that it might have the processing activation means which consisted of fixed hardware circuitry which performs predetermined cryptographic algorithm other than the processing activation means which consisted of recon figure skating rubble circuits, it is effective in low cost-ization being realizable.

[0061] since according to this invention it constituted so that the recon figure skating rubble circuit under un-performing might be chosen and circuitry data might be set up when the processing activation means consisted of two or more recon figure skating rubble circuits — the communication link of a packet — even if working, it is effective in the ability to set up the circuitry data of a recon figure skating rubble circuit.

[0062] According to this invention, the information about the communications partner and cryptographic algorithm of a packet is exchanged, and since it constituted so that the circuitry data corresponding to the cryptographic algorithm to perform might be set as a recon figure skating rubble circuit, there is effectiveness which can enable activation of new cryptographic algorithm after agreeing with a communications partner.

[0063] Since according to this invention it constituted so that it transmitted the identifier which shows the purport which the setting means of a packet transmitting side equips with the recon figure skating rubble circuit to the setting means of a packet receiving side, and the circuitry data corresponding to the cryptographic algorithm to perform might be transmitted to the setting means of a packet receiving side, if the notice of the purport equipped with the recon figure skating rubble circuit from the setting means of that packet receiving side was received, there is effectiveness which can enable activation of new cryptographic algorithm.

[0064] Since according to this invention the setting means of a packet receiving side constituted so that the circuitry data transmitted from the setting means of a packet transmitting side might be received and that circuitry data might be set as a recon figure skating rubble circuit, there is effectiveness which can enable activation of new cryptographic algorithm.

[0065] While a packet transmitting side transmits the identifier which shows a purport equipped with the recon figure skating rubble circuit to a packet receiving side according to this invention If a letter is answered in the notice of the purport which the packet receiving side received the identifier concerned, and equips with the recon figure skating rubble circuit Since it constituted so that the circuitry data corresponding to the cryptographic algorithm which a packet transmitting side performs might be transmitted to a packet receiving side, the packet receiving side might receive the circuitry data concerned and it might be set as a recon figure skating rubble circuit It is effective in the ability to make an addition and modification of cryptographic algorithm easily.

[0066] Since it constituted so that the cryptographic algorithm which a packet transmitting side performs might be transmitted to a packet receiving side and that packet receiving side might receive and set up the cryptographic algorithm concerned when that packet receiving side received the identifier concerned and answered a letter in the notice of the purport which can use a recon figure skating rubble code, while the packet transmitting side transmitted the identifier which shows a recon figure skating rubble code to the packet receiving side according to this invention, it is effective in the ability to make an addition and modification of cryptographic algorithm easily.

[0067] Since according to this invention the cryptographic algorithm transmitted from a packet transmitting side constituted so that it might be the script performed with the script activation engine of a packet receiving side, also in the packet communication device of a script method, it is effective in the ability to make an addition and modification of cryptographic algorithm easily.

[0068] Since according to this invention the cryptographic algorithm transmitted from a packet transmitting side constituted so that it might be the software performed by the microprocessor of a packet receiving side, also in the packet communication device of the software method by the microprocessor, it is effective in the ability to make an addition and modification of cryptographic algorithm easily.

[Translation done.]

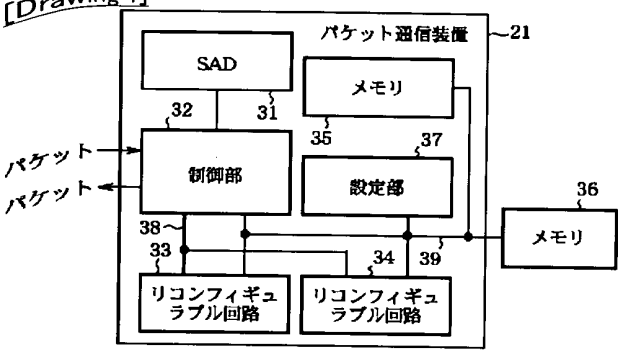
DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the block diagram showing the packet communication device by the gestalt 1 of implementation of this invention.
[Drawing 2] It is the explanatory view showing the contents of storing of memory.
[Drawing 3] It is the processing flow Fig. showing the protocol between packet communication devices.
[Drawing 4] It is the processing flow Fig. showing the protocol between packet communication devices.
[Drawing 5] It is the processing flow Fig. showing the protocol between packet communication devices.
[Drawing 6] It is the block diagram showing the packet communication device by the gestalt 3 of implementation of this invention.
[Drawing 7] It is the processing flow Fig. showing the protocol between packet communication devices.
[Drawing 8] It is the processing flow Fig. showing the protocol between packet communication devices.
[Drawing 9] It is the block diagram showing the conventional packet communication device.
[Drawing 10] It is the processing flow Fig. showing the protocol between packet communication devices.
[Description of Notations]
1 Packet Communication Device, 11 SAD, 12 Control Section, 13 Cipher-Processing Circuit, 14 A cipher-processing circuit, 21, 21a, 21b Packet communication device, 31 control section SAD (algorithm decision means) and 32 (a transmitting means —) 33 A receiving means, an algorithm decision means, 34 35 A recon figure skating rubble circuit (processing activation means), 36 Memory, 37 The setting section (setting means), 38 An encryption circuit bus, 39 A setting bus, 40 Cipher-processing circuit (processing activation means).

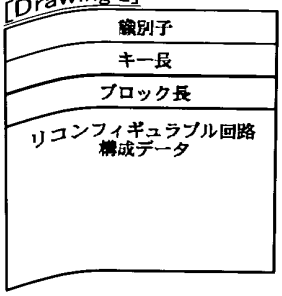
[Translation done.]

DRAWINGS

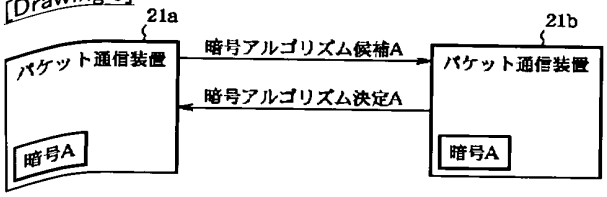
[Drawing 1]



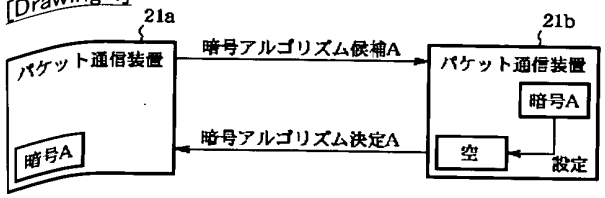
[Drawing 2]



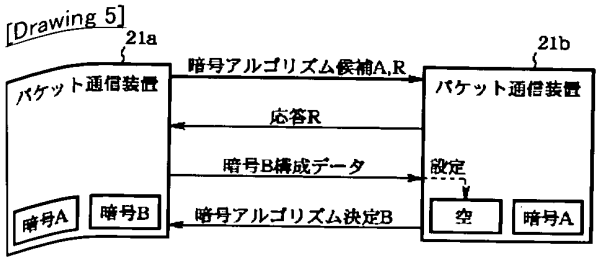
[Drawing 3]



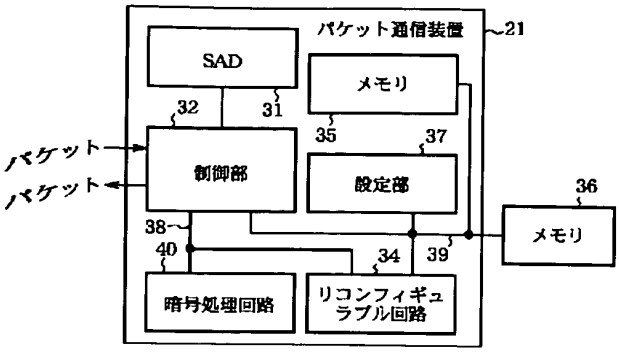
[Drawing 4]



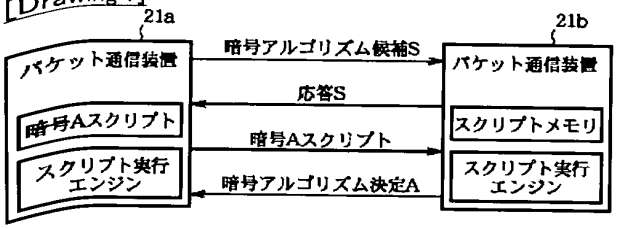
[Drawing 5]



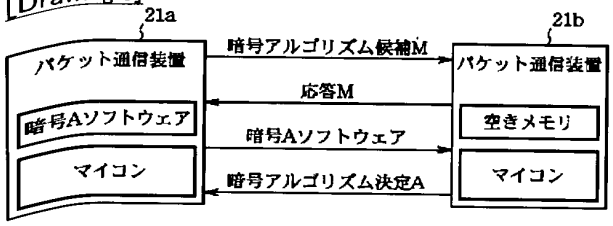
[Drawing 6]



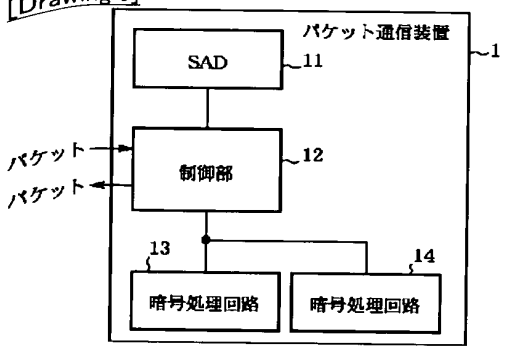
[Drawing 7]



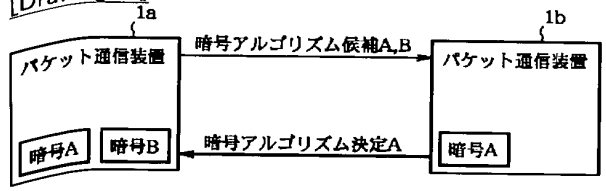
[Drawing 8]



[Drawing 9]



[Drawing 10]



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－198530
（P2003－198530A）
(43)公開日　平成15年７月11日(2003.7.11)

(51)Int.Cl.⁷	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00	６４１	５Ｊ１０４

審査請求　未請求　請求項の数12　ＯＬ　（全９頁）

(21)出願番号　特願2001－390165(P2001－390165)

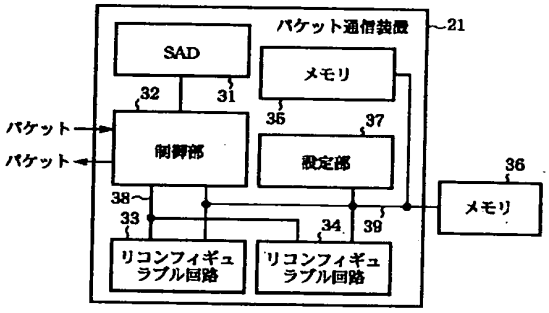
(22)出願日　平成13年12月21日(2001.12.21)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　加藤　守
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100066474
弁理士　田澤　博昭　（外１名）

Ｆターム(参考)　5J104 AA16 AA34 EA04 JA03 JA31 NA01 NA43

(54)【発明の名称】　パケット通信装置及び暗号アルゴリズム設定方法

(57)【要約】
【課題】　送信側と受信側が共に内蔵している暗号アルゴリズム以外は使用することができず、より強力な暗号アルゴリズムが新たに考案されても、新たにハードウェアであるＬＳＩを設計・製造しない限り、使用することができない課題があった。
【解決手段】　パケット通信装置２１がリコンフィギャラブル回路３３，３４の回路構成データを設定する設定部３７を内蔵するように構成した。これにより、暗号アルゴリズムの追加や変更を簡単に行うことができる効果を奏する。



【特許請求の範囲】

【請求項１】　パケットの宛先を確認し、その宛先に応じて暗号アルゴリズムを決定するアルゴリズム決定手段と、上記アルゴリズム決定手段により決定された暗号アルゴリズムを実行して、そのパケットに対する暗号化処理を行う処理実行手段と、上記処理実行手段による暗号化後のパケットを送信する送信手段とを備えたパケット通信装置において、リコンフィギャラブル回路を用いて上記処理実行手段を構成し、上記リコンフィギャラブル回路の回路構成データを設定する設定手段を設けたことを特徴とするパケット通信装置。

【請求項２】　暗号化されたパケットを受信する受信手段と、上記受信手段により受信されたパケットの送信元を確認し、その送信元に応じて暗号アルゴリズムを決定するアルゴリズム決定手段と、上記アルゴリズム決定手段により決定された暗号アルゴリズムを実行して、そのパケットに対する復号化処理を行う処理実行手段とを備えたパケット通信装置において、リコンフィギャラブル回路を用いて上記処理実行手段を構成し、上記リコンフィギャラブル回路の回路構成データを設定する設定手段を設けたことを特徴とするパケット通信装置。

【請求項３】　設定手段は、リコンフィギャラブル回路の回路構成データを設定する際、暗号鍵のキー長及び暗号化又は復号化ブロックのビット数を登録することを特徴とする請求項１または請求項２記載のパケット通信装置。

【請求項４】　リコンフィギャラブル回路から構成された処理実行手段の他に、所定の暗号アルゴリズムを実行する固定ハードウェア回路から構成された処理実行手段を備えていることを特徴とする請求項１または請求項２記載のパケット通信装置。

【請求項５】　設定手段は、処理実行手段が複数のリコンフィギャラブル回路から構成されている場合、未実行中のリコンフィギャラブル回路を選択して回路構成データを設定することを特徴とする請求項１または請求項２記載のパケット通信装置。

【請求項６】　設定手段は、パケットの通信相手と暗号アルゴリズムに関する情報を交換して、実行する暗号アルゴリズムに対応する回路構成データをリコンフィギャラブル回路に設定することを特徴とする請求項１から請求項５のうちのいずれか１項記載のパケット通信装置。

【請求項７】　パケット送信側の設定手段は、リコンフィギャラブル回路を備えている旨を示す識別子をパケット受信側の設定手段に送信し、そのパケット受信側の設定手段からリコンフィギャラブル回路を備えている旨の通知を受けると、実行する暗号アルゴリズムに対応する回路構成データをパケット受信側の設定手段に送信することを特徴とする請求項６記載のパケット通信装置。

【請求項８】　パケット受信側の設定手段は、パケット送信側の設定手段から送信された回路構成データを受信し、その回路構成データをリコンフィギャラブル回路に設定することを特徴とする請求項７記載のパケット通信装置。

【請求項９】　パケット送信側がリコンフィギャラブル回路を備えている旨を示す識別子をパケット受信側に送信する一方、そのパケット受信側が当該識別子を受信してリコンフィギャラブル回路を備えている旨の通知を返信すると、上記パケット送信側が実行する暗号アルゴリズムに対応する回路構成データを上記パケット受信側に送信し、そのパケット受信側が当該回路構成データを受信してリコンフィギャラブル回路に設定する暗号アルゴリズム設定方法。

【請求項１０】　パケット送信側がリコンフィギャラブル暗号を示す識別子をパケット受信側に送信する一方、そのパケット受信側が当該識別子を受信してリコンフィギャラブル暗号の使用が可能である旨の通知を返信すると、上記パケット送信側が実行する暗号アルゴリズムを上記パケット受信側に送信し、そのパケット受信側が当該暗号アルゴリズムを受信して設定する暗号アルゴリズム設定方法。

【請求項１１】　パケット送信側から送信される暗号アルゴリズムが、パケット受信側のスクリプト実行エンジンにより実行されるスクリプトであることを特徴とする請求項１０記載の暗号アルゴリズム設定方法。

【請求項１２】　パケット送信側から送信される暗号アルゴリズムが、パケット受信側のマイクロプロセッサにより実行されるソフトウェアであることを特徴とする請求項１０記載の暗号アルゴリズム設定方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、暗号アルゴリズムの追加や変更を行うことができるパケット通信装置及び暗号アルゴリズム設定方法に関するものである。

【０００２】

【従来の技術】インターネット等の通信インフラの発達により、企業内や企業間等の専用線による通信に代わって、ＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）が注目されている。ＶＰＮは暗号化技術により、インターネットを仮想的な専用線として利用可能にする技術であり、ＩＰＳＥＣ（Ｓｅｃｕｒｉｔｙ　Ａｒｃｈｉｔｅｃｔｕｒｅ　ｆｏｒ　Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）が現在の標準となっている。ＩＰＳＥＣでは、使用する暗号アルゴリズムが固定されておらず、必須の暗号アルゴリズムＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）などに加えて任意のアルゴリズムのサポートが可能である。

【０００３】図９は従来のパケット通信装置を示す構成図であり、図において、１は例えばネットワークセキュリティＬＳＩであるパケット通信装置、１１は通信相手が実行可能な暗号アルゴリズムを示す情報等を格納する

ＳＡＤ（ＳｅｃｕｒｉｔｙＡｓｓｏｃｉａｔｉｏｎ　Ｄａｔａｂａｓｅ）、１２はパケットの送受信を実行するとともに、暗号処理回路１３，１４を制御する制御部、１３は暗号アルゴリズムＡを実行して、パケットに対する暗号化処理又は復号化処理を実行する暗号処理回路、１４は暗号アルゴリズムＢを実行して、パケットに対する暗号化処理又は復号化処理を実行する暗号処理回路である。なお、図９の例では、パケット通信装置が２つの暗号処理回路を内蔵するものについて示しているが、これに限るものではなく、１つの暗号処理回路のみを内蔵していてもよいし、３以上の暗号処理回路を内蔵していてもよい。

【０００４】次に動作について説明する。ここでは、図１０に示すように、暗号アルゴリズムＡ，Ｂの実行が可能なパケット通信装置１ａがパケットを暗号化して送信し、暗号アルゴリズムＡの実行が可能なパケット通信装置１ｂがパケットを受信して復号化するものについて説明する。

【０００５】まず、パケット通信装置１ａの制御部１２は、パケットの暗号化通信を開始するに際して、実行が可能な暗号アルゴリズムを受信側のパケット通信装置１ｂに認識させるため、暗号アルゴリズムＡ，Ｂにそれぞれ割り当てられている識別子をパケット通信装置１ｂに送信する。

【０００６】パケット通信装置１ｂの制御部１２は、パケット通信装置１ａから暗号アルゴリズムＡの識別子と暗号アルゴリズムＢの識別子を受信すると、パケット通信装置１ａが実行可能な暗号アルゴリズムが暗号アルゴリズムＡ，Ｂであると認識する。そして、パケット通信装置１ｂの制御部１２は、暗号アルゴリズムＡ，Ｂのうち、自己が実行可能な暗号アルゴリズムが暗号アルゴリズムＡであるので、暗号アルゴリズムＡの使用を許可する決定情報をパケット通信装置１ａに送信するとともに、パケット通信装置１ａのアドレス等と関連付けて当該決定情報をＳＡＤ１１に格納する。

【０００７】パケット通信装置１ａの制御部１２は、パケット通信装置１ｂから暗号アルゴリズムＡの使用を許可する決定情報を受信すると、パケット通信装置１ｂのアドレス等と関連付けて当該決定情報をＳＡＤ１１に格納する。そして、パケット通信装置１ａの制御部１２は、パケット通信装置１ｂに送信する平文のパケットを入力すると、そのパケットに付加されているアドレス等をキーにしてＳＡＤ１１から決定情報を取得し、その決定情報から使用する暗号アルゴリズムを認識する。この例では、暗号アルゴリズムＡを使用するものと認識する。

【０００８】パケット通信装置１ａの制御部１２は、使用する暗号アルゴリズムが暗号アルゴリズムＡであるので、暗号アルゴリズムＡを内蔵している暗号処理回路１３に対して平文のパケットを出力する。これにより、暗号処理回路１３は、暗号アルゴリズムＡを実行して、平文のパケットに対する暗号化処理を実施し、暗号化後のパケットを制御部１２に出力する。パケット通信装置１ａの制御部１２は、暗号化後のパケットをパケット通信装置１ｂに送信する。

【０００９】パケット通信装置１ｂの制御部１２は、パケット通信装置１ａから暗号化後のパケットを受信すると、そのパケットに付加されているアドレス等をキーにしてＳＡＤ１１から決定情報を取得し、その決定情報から使用する暗号アルゴリズムを認識する。この例では、暗号アルゴリズムＡを使用するものと認識する。

【００１０】パケット通信装置１ｂの制御部１２は、使用する暗号アルゴリズムが暗号アルゴリズムＡであるので、暗号アルゴリズムＡを内蔵している暗号処理回路１３に対して暗号化後のパケットを出力する。これにより、暗号処理回路１３は、暗号アルゴリズムＡを実行して、暗号化後のパケットに対する復号化処理を実施し、平文のパケットを制御部１２に出力する。パケット通信装置１ｂの制御部１２は、平文のパケットを外部出力する。

【００１１】

【発明が解決しようとする課題】従来のパケット通信装置は以上のように構成されているので、送信側と受信側が共に内蔵している暗号アルゴリズム以外は使用することができず、より強力な暗号アルゴリズムが新たに考案されても、新たにハードウェアであるＬＳＩを設計・製造しない限り、使用することができない課題があった。

【００１２】なお、特開平１０－２５７１２０号公報には、パケット通信装置がパケットの暗号化通信を実行する際、ネットワークに接続されているデータベースから暗号アルゴリズムに相当するスクリプトを取得し、パケット通信装置のスクリプト実行エンジンが当該スクリプトを実行する技術が開示されている。しかし、この場合、特定のパケット通信装置間でのみ使用されるべき秘匿性の高い暗号アルゴリズムがデータベースに登録されるため、サーバ管理組織の高いモラルが求められると同時に、内部犯罪等により暗号アルゴリズムが流出する可能性があるなどの問題がある。また、スクリプト実行エンジンがスクリプトの意味を解釈しながら暗号化処理等を実施する必要があるため、ハードウェアが実装されたパケット通信装置と比べて暗号化処理等の速度が遅くなる問題もある。

【００１３】この発明は上記のような課題を解決するためになされたもので、暗号アルゴリズムの追加や変更を簡単に行うことができるパケット通信装置及び暗号アルゴリズム設定方法を得ることを目的とする。

【００１４】

【課題を解決するための手段】この発明に係るパケット通信装置は、パケットを暗号化して送信するに際して、リコンフィギャラブル回路の回路構成データを設定する

設定手段を設けたものである。

【００１５】この発明に係るパケット通信装置は、パケットを受信して復号化するに際して、リコンフィギャラブル回路の回路構成データを設定する設定手段を設けたものである。

【００１６】この発明に係るパケット通信装置は、リコンフィギャラブル回路の回路構成データを設定する際、暗号鍵のキー長及び暗号化又は復号化ブロックのビット数を登録するようにしたものである。

【００１７】この発明に係るパケット通信装置は、リコンフィギャラブル回路から構成された処理実行手段の他に、所定の暗号アルゴリズムを実行する固定ハードウェア回路から構成された処理実行手段を備えるようにしたものである。

【００１８】この発明に係るパケット通信装置は、処理実行手段が複数のリコンフィギャラブル回路から構成されている場合、未実行中のリコンフィギャラブル回路を選択して回路構成データを設定するようにしたものである。

【００１９】この発明に係るパケット通信装置は、パケットの通信相手と暗号アルゴリズムに関する情報を交換して、実行する暗号アルゴリズムに対応する回路構成データをリコンフィギャラブル回路に設定するようにしたものである。

【００２０】この発明に係るパケット通信装置は、パケット送信側の設定手段がリコンフィギャラブル回路を備えている旨を示す識別子をパケット受信側の設定手段に送信し、そのパケット受信側の設定手段からリコンフィギャラブル回路を備えている旨の通知を受けると、実行する暗号アルゴリズムに対応する回路構成データをパケット受信側の設定手段に送信するようにしたものである。

【００２１】この発明に係るパケット通信装置は、パケット受信側の設定手段が、パケット送信側の設定手段から送信された回路構成データを受信し、その回路構成データをリコンフィギャラブル回路に設定するようにしたものである。

【００２２】この発明に係る暗号アルゴリズム設定方法は、パケット送信側がリコンフィギャラブル回路を備えている旨を示す識別子をパケット受信側に送信する一方、そのパケット受信側が当該識別子を受信してリコンフィギャラブル回路を備えている旨の通知を返信すると、パケット送信側が実行する暗号アルゴリズムに対応する回路構成データをパケット受信側に送信し、そのパケット受信側が当該回路構成データを受信してリコンフィギャラブル回路に設定するようにしたものである。

【００２３】この発明に係る暗号アルゴリズム設定方法は、パケット送信側がリコンフィギャラブル暗号を示す識別子をパケット受信側に送信する一方、そのパケット受信側が当該識別子を受信してリコンフィギャラブル暗号の使用が可能である旨の通知を返信すると、パケット送信側が実行する暗号アルゴリズムをパケット受信側に送信し、そのパケット受信側が当該暗号アルゴリズムを受信して設定するようにしたものである。

【００２４】この発明に係る暗号アルゴリズム設定方法は、パケット送信側から送信される暗号アルゴリズムが、パケット受信側のスクリプト実行エンジンにより実行されるスクリプトであるようにしたものである。

【００２５】この発明に係る暗号アルゴリズム設定方法は、パケット送信側から送信される暗号アルゴリズムが、パケット受信側のマイクロプロセッサにより実行されるソフトウェアであるようにしたものである。

【００２６】

【発明の実施の形態】以下、この発明の実施の一形態を説明する。

実施の形態１．図１はこの発明の実施の形態１によるパケット通信装置を示す構成図であり、図において、２１は例えばネットワークセキュリティＬＳＩであるパケット通信装置、３１は通信相手が実行可能な暗号アルゴリズムを示す情報等を格納するＳＡＤ、３２はパケットの送受信を実行するとともに、パケットの宛先又は送信元を確認し、その宛先又は送信元に応じて暗号アルゴリズムを決定する制御部（送信手段、受信手段）である。なお、ＳＡＤ３１及び制御部３２からアルゴリズム決定手段が構成されている。

【００２７】３３，３４は制御部３２により決定された暗号アルゴリズムを実行して、そのパケットに対する暗号化処理又は復号化処理を行うリコンフィギャラブル回路（処理実行手段）であり、リコンフィギャラブル回路３３，３４は例えばＦＰＧＡやＣＰＬＤなどの技術を使用して構成される。３５，３６は暗号鍵のキー長及び暗号化ブロックのビット数やリコンフィギャラブル回路３３，３４の回路構成データを格納するメモリ、３７はリコンフィギャラブル回路３３，３４の回路構成データを設定する設定部（設定手段）、３８は制御部３２とリコンフィギュラブル回路３３，３４間を接続し、暗号化の対象となるパケットを伝送する暗号化回路バス、３９は制御部３２、リコンフィギュラブル回路３３，３４、設定部３７及びメモリ３５，３６間を接続し、リコンフィギャラブル回路３３，３４の回路構成データ等を伝送する設定バスである。

【００２８】なお、メモリ３５，３６としては、例えば、フラッシュメモリ、ＥＥＰＲＯＭ、マスクＲＯＭなどの不揮発性メモリや、ＲＡＭなどの揮発性メモリが使用可能である。省面積化のためにメモリ３５のようにＬＳＩに内蔵してもよいし、多くの暗号アルゴリズムを選択して実装可能にするために、メモリ３６のように外付けとしてもよい。また、その両方を実装することにより、例えば、標準の暗号アルゴリズムを内部マスクＲＯＭで固定的に保持し、オプションの暗号アルゴリズムを

外付けフラッシュメモリやコンパクトフラッシュ（Ｒ）などのメモリカードで提供することも可能である。また、図１の例では、パケット通信装置が２つのリコンフィギャラブル回路を内蔵するものについて示しているが、これに限るものではなく、１つのリコンフィギャラブル回路のみを内蔵していてもよいし、３以上のリコンフィギャラブル回路を内蔵していてもよい。

【００２９】次に動作について説明する。まず、パケット通信装置２１が実行する暗号アルゴリズムの変更や追加を行う場合、設定部３７は、ＬＳＩがリセットされると、メモリ３５又はメモリ３６に格納されているリコンフィギャラブル回路の回路構成データを取得する。なお、回路構成データは、図２に示すように、対応する暗号アルゴリズムを示す識別子、暗号鍵のキー長、暗号化ブロックのビット数などの属性情報と一緒に格納されている。

【００３０】そして、設定部３７は、リコンフィギャラブル回路の回路構成データを取得すると、その回路構成データを例えばリコンフィギャラブル回路３３に設定する。これにより、その回路構成データが例えば暗号アルゴリズムＢの回路構成データであれば、以後、リコンフィギャラブル回路３３は、暗号アルゴリズムＢの実行が可能になる。

【００３１】なお、パケット通信装置２１の制御部３２が通信動作を実行している場合、設定部３７は、メモリ３５又はメモリ３６から回路構成データを取得すると、リコンフィギャラブル回路３３，３４のうち、現在実行していない方のリコンフィギャラブル回路を選択し、そのリコンフィギャラブル回路に対して回路構成データを設定する。

【００３２】ここで、制御部３２は、リコンフィギャラブル回路３３に対してパケットの暗号化処理や復号化処理を依頼する際、暗号化回路バス３８を介して、パケットをリコンフィギャラブル回路３３に転送するが、メモリ３５又はメモリ３６に格納されている暗号鍵のキー長や暗号化ブロックのビット数の読み込みを行う。そして、仮に、暗号鍵のキー長や暗号化ブロックのビット数が暗号化回路バス３８のビット幅よりも大きいときには、複数回に分けて転送を行う。例えば、暗号化回路バス３８のビット幅が６４ビットで、キー長が１２８ビットの場合、暗号鍵を２回に分けて転送する。このことにより、キー長やブロックのビット数が異なる任意の暗号アルゴリズムをリコンフィギュラブル回路に実装することができる。

【００３３】次に、図３に示すように、標準的な暗号アルゴリズムＡ（例えば、ＤＥＳ）の実行が可能なパケット通信装置２１ａが、暗号アルゴリズムＡの実行が可能なパケット通信装置２１ｂにパケットを送信する場合の動作を説明する（以下、動作例１と称する）。

【００３４】まず、パケット通信装置２１ａの制御部３２は、実行が可能な暗号アルゴリズムを受信側のパケット通信装置２１ｂに認識させるため、暗号アルゴリズムＡに割り当てられている識別子Ａをパケット通信装置２１ｂに送信する。パケット通信装置２１ｂの制御部３２は、パケット通信装置２１ａから暗号アルゴリズムＡの識別子Ａを受信すると、自身が暗号アルゴリズムＡの実行が可能であるため、暗号アルゴリズムＡの使用を許可する決定情報をパケット通信装置２１ａに送信するとともに、パケット通信装置２１ａのアドレス等と関連付けて当該決定情報をＳＡＤ３１に格納する。

【００３５】パケット通信装置２１ａの制御部３２は、パケット通信装置２１ｂから暗号アルゴリズムＡの使用を許可する決定情報を受信すると、パケット通信装置２１ｂのアドレス等と関連付けて当該決定情報をＳＡＤ３１に格納する。そして、パケット通信装置２１ａの制御部３２は、パケット通信装置２１ｂに送信する平文のパケットを入力すると、そのパケットに付加されているアドレス等をキーにしてＳＡＤ３１から決定情報を取得し、その決定情報から使用する暗号アルゴリズムを認識する。この例では、暗号アルゴリズムＡを使用するものと認識する。

【００３６】パケット通信装置２１ａの制御部３２は、使用する暗号アルゴリズムが暗号アルゴリズムＡであるので、暗号アルゴリズムＡの実行が可能なリコンフィギュラブル回路（ここでは、説明の便宜上、リコンフィギュラブル回路３３が暗号アルゴリズムＡを実行することができるものとする）に対して平文のパケットを出力する。これにより、リコンフィギュラブル回路３３は、暗号アルゴリズムＡを実行して、平文のパケットに対する暗号化処理を実施し、暗号化後のパケットを制御部３２に出力する。パケット通信装置２１ａの制御部３２は、暗号化後のパケットをパケット通信装置２１ｂに送信する。

【００３７】パケット通信装置２１ｂの制御部３２は、パケット通信装置２１ａから暗号化後のパケットを受信すると、そのパケットに付加されているアドレス等をキーにしてＳＡＤ３１から決定情報を取得し、その決定情報から使用する暗号アルゴリズムを認識する。この例では、暗号アルゴリズムＡを使用するものと認識する。

【００３８】パケット通信装置２１ｂの制御部３２は、使用する暗号アルゴリズムが暗号アルゴリズムＡであるので、暗号アルゴリズムＡの実行が可能なリコンフィギュラブル回路（ここでは、説明の便宜上、リコンフィギュラブル回路３３が暗号アルゴリズムＡを実行することができるものとする）に対して暗号化後のパケットを出力する。これにより、リコンフィギュラブル回路３３は、暗号アルゴリズムＡを実行して、暗号化後のパケットに対する復号化処理を実施し、平文のパケットを制御部３２に出力する。パケット通信装置２１ｂの制御部３２は、平文のパケットを外部出力する。

【００３９】次に、図４に示すように、標準的な暗号アルゴリズムＡの実行が可能なパケット通信装置２１ａが、暗号アルゴリズムＡの回路構成データがリコンフィギュラブル回路に対して未設定のパケット通信装置２１ｂにパケットを送信する場合の動作を説明する（以下、動作例２と称する）。ただし、暗号アルゴリズムＡは、標準的な暗号（例えば、ＤＥＳ）であるため、メモリ３５には予め暗号アルゴリズムＡの回路構成データが格納されているものとする。

【００４０】まず、パケット通信装置２１ａの制御部３２は、実行が可能な暗号アルゴリズムを受信側のパケット通信装置２１ｂに認識させるため、暗号アルゴリズムＡに割り当てられている識別子Ａをパケット通信装置２１ｂに送信する。パケット通信装置２１ｂの制御部３２は、パケット通信装置２１ａから暗号アルゴリズムＡの識別子Ａを受信すると、内蔵するリコンフィギュラブル回路３３に暗号アルゴリズムＡの回路構成データが設定されていないため、暗号アルゴリズムＡの回路構成データの設定を設定部３７に要求する。

【００４１】これにより、パケット通信装置２１ｂの設定部３７は、メモリ３５から暗号アルゴリズムＡの回路構成データを取得し、その回路構成データをリコンフィギュラブル回路３３に設定する。パケット通信装置２１ｂの制御部３２は、設定部３７による回路構成データの設定が完了すると、暗号アルゴリズムＡの使用を許可する決定情報をパケット通信装置２１ａに送信するとともに、パケット通信装置２１ａのアドレス等と関連付けて当該決定情報をＳＡＤ３１に格納する。

【００４２】パケット通信装置２１ａの制御部３２は、パケット通信装置２１ｂから暗号アルゴリズムＡの使用を許可する決定情報を受信すると、パケット通信装置２１ｂのアドレス等と関連付けて当該決定情報をＳＡＤ３１に格納する。以下の通信動作は、上記の動作例１と同様であるため説明を省略する。

【００４３】次に、図５に示すように、標準的な暗号アルゴリズムＡと新たに考案された暗号アルゴリズムＢの実行が可能なパケット通信装置２１ａが、暗号アルゴリズムＡの実行が可能なパケット通信装置２１ｂにパケットを送信する場合の動作を説明する（以下、動作例３と称する）。ただし、暗号アルゴリズムＢは、新たに考案された暗号であるため、メモリ３５には暗号アルゴリズムＢの回路構成データが格納されていないものとする。

【００４４】まず、パケット通信装置２１ａの制御部３２は、実行が可能な暗号アルゴリズムを受信側のパケット通信装置２１ｂに認識させるため、暗号アルゴリズムＡに割り当てられている識別子Ａと、自身がリコンフィギュラブル回路を備えている旨を示す識別子Ｒ（または、リコンフィギュラブル暗号の使用が可能である旨を示す識別子）をパケット通信装置２１ｂに送信する。パケット通信装置２１ｂの制御部３２は、パケット通信装置２１ａから暗号アルゴリズムＡの識別子Ａの他に識別子Ｒを受信すると、自身もリコンフィギュラブル回路を備えている旨の応答Ｒ（または、自身もリコンフィギュラブル暗号の使用が可能である旨の応答）をパケット通信装置２１ａに送信する。

【００４５】ただし、パケット通信装置２１ｂがリコンフィギュラブル回路を備えていない場合には、暗号アルゴリズムＡの使用を許可する決定情報をパケット通信装置２１ａに送信する。この場合、以下の通信動作は、上記の動作例１と同様であるため説明を省略する。

【００４６】パケット通信装置２１ａの制御部３２は、パケット通信装置２１ｂから自身もリコンフィギュラブル回路を備えている旨の応答Ｒを受信すると、新たに考案された暗号の使用を可能にするため、暗号アルゴリズムＢの回路構成データをパケット通信装置２１ｂに送信する。パケット通信装置２１ｂの制御部３２は、パケット通信装置２１ａから暗号アルゴリズムＢの回路構成データを受信すると、暗号アルゴリズムＢの回路構成データを空いているリコンフィギュラブル回路（例えば、リコンフィギュラブル回路３４）に設定する。

【００４７】なお、空いているリコンフィギュラブル回路が無い場合には、例えば、最も使用頻度の低い暗号アルゴリズムの回路構成データを実装するリコンフィギュラブル回路を無効化するなど、一般的に考えられる無効化アルゴリズムに従って、いずれか一つのリコンフィギュラブル回路を強制的に空きにして使用できるようにする。

【００４８】パケット通信装置２１ｂの制御部３２は、回路構成データの設定が完了すると、暗号アルゴリズムＢの使用を許可する決定情報をパケット通信装置２１ａに送信するとともに、パケット通信装置２１ａのアドレス等と関連付けて当該決定情報をＳＡＤ３１に格納する。

【００４９】パケット通信装置２１ａの制御部３２は、パケット通信装置２１ｂから暗号アルゴリズムＢの使用を許可する決定情報を受信すると、パケット通信装置２１ｂのアドレス等と関連付けて当該決定情報をＳＡＤ３１に格納する。以下の通信動作は、上記の動作例１と同様であるため説明を省略する。

【００５０】以上で明らかなように、この実施の形態１によれば、リコンフィギャラブル回路３３，３４の回路構成データを設定する設定部３７を設けるように構成したので、暗号アルゴリズムの追加や変更を簡単に行うことができる効果がある。また、送信側と受信側が一対一の通信によって暗号アルゴリズムの回路構成データを伝送し、従来例のようにデータベースに暗号アルゴリズムを登録する必要がないので、暗号アルゴリズムの秘匿性を確保することができる効果がある。なお、リコンフィギャラブル回路３３，３４はハードウェアであるので、従来のスクリプト実行エンジンのような処理速度の遅延

が問題になることはない。

【００５１】この実施の形態１では、特に言及していないが、複数のパケット通信装置がネットワークに接続されているような場合には、複数のパケット通信装置に対してＩＰアドレスを割り振り、送信側がパケットにＩＰアドレスを付加して送信する際、そのパケットに暗号アルゴリズムの回路構成データを含めて送信し、受信側が当該回路構成データをメモリ３５に格納するようにする。これにより、あるパケット通信装置が他のパケット通信装置に対して、暗号アルゴリズムの追加を行うことができる。

【００５２】実施の形態２．上記実施の形態１では、特に言及していないが、実行可能な暗号アルゴリズムを示す識別子や暗号アルゴリズムの回路構成データ等を伝送する際、その識別子や回路構成データを例えば標準的な暗号化アルゴリズムによって暗号化して伝送するようにしてもよい。また、上記実施の形態１では、暗号アルゴリズムの回路構成データを設定するものについて示したが、送信側が暗号鍵のキー長や暗号化ブロックのビット数等の属性情報を受信側に送信し、その属性情報を受信側のメモリ３５に格納するようにしてもよい。これにより、暗号鍵のキー長や暗号化ブロックのビット数等も変更することができる。

【００５３】実施の形態３．図６はこの発明の実施の形態３によるパケット通信装置を示す構成図であり、図において、図１と同一符号は同一または相当部分を示すので説明を省略する。４０は所定の暗号アルゴリズムを実行する固定ハードウェア回路である暗号処理回路（処理実行手段）である。

【００５４】次に動作について説明する。上記実施の形態１では、複数のリコンフィギャラブル回路を搭載するものについて示したが、図６に示すように、リコンフィギャラブル回路３４の他に暗号処理回路４０を搭載するようにしてもよい。これにより、ＩＰＳＥＣ等の規格にて実装することが必須となっている暗号アルゴリズムを最小のハードウェア量で実装することが可能となり（当該暗号アルゴリズムを暗号処理回路４０に実装する）、低コスト化を実現することができる効果を奏する。

【００５５】実施の形態４．上記実施の形態１では、暗号アルゴリズムの回路構成データを送信するものについて示したが、図７に示すように、受信側であるパケット通信装置２１ｂのスクリプト実行エンジンが暗号アルゴリズムを実行する場合には、送信側であるパケット通信装置２１ａから送信される暗号アルゴリズムが、そのスクリプト実行エンジンにより実行されるスクリプトであるようにしてもよい。これにより、スクリプト方式のパケット通信装置においても、上記実施の形態１と同様の効果を奏することができる。

【００５６】実施の形態５．上記実施の形態１では、暗号アルゴリズムの回路構成データを送信するものについて示したが、図８に示すように、受信側であるパケット通信装置２１ｂのマイクロプロセッサが暗号アルゴリズムを実行する場合には、送信側であるパケット通信装置２１ａから送信される暗号アルゴリズムが、そのマイクロプロセッサにより実行されるソフトウェアであるようにしてもよい。これにより、マイクロプロセッサによるソフトウェア方式のパケット通信装置においても、上記実施の形態１と同様の効果を奏することができる。

【００５７】

【発明の効果】以上のように、この発明によれば、パケットを暗号化して送信するに際して、リコンフィギャラブル回路の回路構成データを設定する設定手段を設けるように構成したので、暗号アルゴリズムの追加や変更を簡単に行うことができる効果がある。

【００５８】この発明によれば、パケットを受信して復号化するに際して、リコンフィギャラブル回路の回路構成データを設定する設定手段を設けるように構成したので、暗号アルゴリズムの追加や変更を簡単に行うことができる効果がある。

【００５９】この発明によれば、リコンフィギャラブル回路の回路構成データを設定する際、暗号鍵のキー長及び暗号化又は復号化ブロックのビット数を登録するように構成したので、暗号鍵のキー長や暗号化又は復号化ブロックのビット数についても簡単に追加や変更を行うことができる効果がある。

【００６０】この発明によれば、リコンフィギャラブル回路から構成された処理実行手段の他に、所定の暗号アルゴリズムを実行する固定ハードウェア回路から構成された処理実行手段を備えるように構成したので、低コスト化を実現することができる効果がある。

【００６１】この発明によれば、処理実行手段が複数のリコンフィギャラブル回路から構成されている場合、未実行中のリコンフィギャラブル回路を選択して回路構成データを設定するように構成したので、パケットの通信動作中であっても、リコンフィギャラブル回路の回路構成データを設定することができる効果がある。

【００６２】この発明によれば、パケットの通信相手と暗号アルゴリズムに関する情報を交換して、実行する暗号アルゴリズムに対応する回路構成データをリコンフィギャラブル回路に設定するように構成したので、通信相手と合意の上で新たな暗号アルゴリズムの実行を可能にすることができる効果がある。

【００６３】この発明によれば、パケット送信側の設定手段がリコンフィギャラブル回路を備えている旨を示す識別子をパケット受信側の設定手段に送信し、そのパケット受信側の設定手段からリコンフィギャラブル回路を備えている旨の通知を受けると、実行する暗号アルゴリズムに対応する回路構成データをパケット受信側の設定手段に送信するように構成したので、新たな暗号アルゴリズムの実行を可能にすることができる効果がある。

【００６４】この発明によれば、パケット受信側の設定手段が、パケット送信側の設定手段から送信された回路構成データを受信し、その回路構成データをリコンフィギャラブル回路に設定するように構成したので、新たな暗号アルゴリズムの実行を可能にすることができる効果がある。

【００６５】この発明によれば、パケット送信側がリコンフィギャラブル回路を備えている旨を示す識別子をパケット受信側に送信する一方、そのパケット受信側が当該識別子を受信してリコンフィギャラブル回路を備えている旨の通知を返信すると、パケット送信側が実行する暗号アルゴリズムに対応する回路構成データをパケット受信側に送信し、そのパケット受信側が当該回路構成データを受信してリコンフィギャラブル回路に設定するように構成したので、暗号アルゴリズムの追加や変更を簡単に行うことができる効果がある。

【００６６】この発明によれば、パケット送信側がリコンフィギャラブル暗号を示す識別子をパケット受信側に送信する一方、そのパケット受信側が当該識別子を受信してリコンフィギャラブル暗号の使用が可能である旨の通知を返信すると、パケット送信側が実行する暗号アルゴリズムをパケット受信側に送信し、そのパケット受信側が当該暗号アルゴリズムを受信して設定するように構成したので、暗号アルゴリズムの追加や変更を簡単に行うことができる効果がある。

【００６７】この発明によれば、パケット送信側から送信される暗号アルゴリズムが、パケット受信側のスクリプト実行エンジンにより実行されるスクリプトであるように構成したので、スクリプト方式のパケット通信装置においても、暗号アルゴリズムの追加や変更を簡単に行うことができる効果がある。

【００６８】この発明によれば、パケット送信側から送信される暗号アルゴリズムが、パケット受信側のマイクロプロセッサにより実行されるソフトウェアであるよう＊に構成したので、マイクロプロセッサによるソフトウェア方式のパケット通信装置においても、暗号アルゴリズムの追加や変更を簡単に行うことができる効果がある。

【図面の簡単な説明】

【図１】　この発明の実施の形態１によるパケット通信装置を示す構成図である。

【図２】　メモリの格納内容を示す説明図である。

【図３】　パケット通信装置間のプロトコルを示す処理フロー図である。

【図４】　パケット通信装置間のプロトコルを示す処理フロー図である。

【図５】　パケット通信装置間のプロトコルを示す処理フロー図である。

【図６】　この発明の実施の形態３によるパケット通信装置を示す構成図である。

【図７】　パケット通信装置間のプロトコルを示す処理フロー図である。

【図８】　パケット通信装置間のプロトコルを示す処理フロー図である。

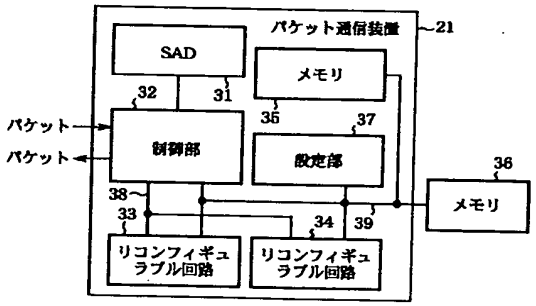
【図９】　従来のパケット通信装置を示す構成図である。

【図１０】　パケット通信装置間のプロトコルを示す処理フロー図である。

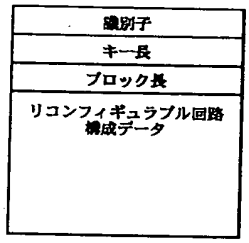
【符号の説明】

１　パケット通信装置、１１　ＳＡＤ、１２　制御部、１３　暗号処理回路、１４　暗号処理回路、２１，２１ａ，２１ｂ　パケット通信装置、３１　ＳＡＤ（アルゴリズム決定手段）、３２　制御部（送信手段、受信手段、アルゴリズム決定手段）、３３，３４　リコンフィギャラブル回路（処理実行手段）、３５，３６　メモリ、３７　設定部（設定手段）、３８　暗号化回路バス、３９　設定バス、４０　暗号処理回路（処理実行手段）。

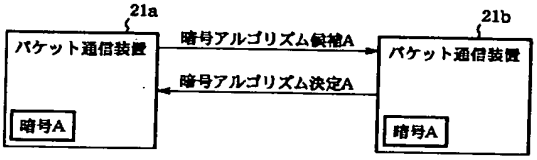
【図１】



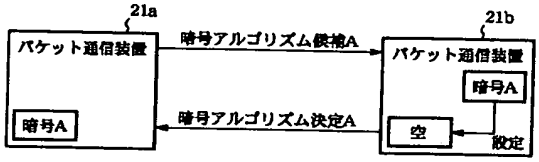
【図２】



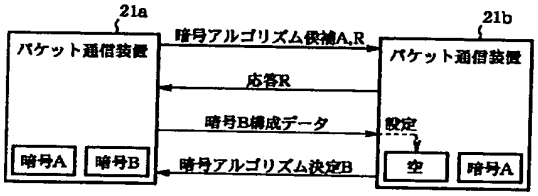
【図３】



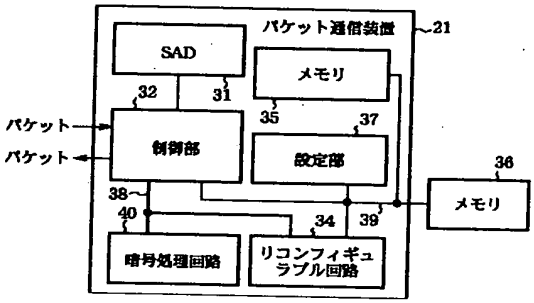
【図４】



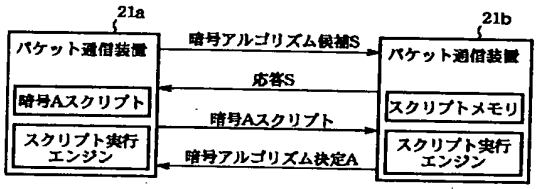
【図５】



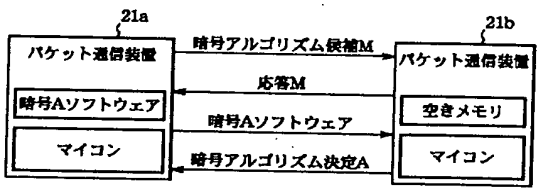
【図６】



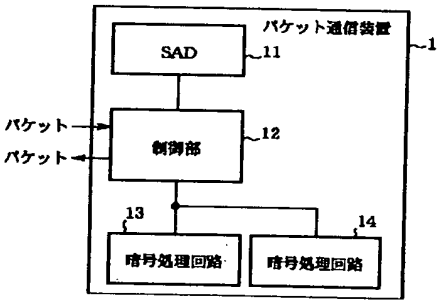
【図７】



【図８】



【図９】



【図１０】